Gröbner-bases

Jesse Vogel

Universiteit Leiden

1 maart, 2023

Ideale lidmaatschapsprobleem

Zij $R = \mathbb{Q}[x_1, x_2, \ldots, x_n]$ en $I = (g_1, g_2, \ldots, g_k)$ een ideaal.

Gegeven een polynoom $f \in R$, is $f \in I$?

Voorbeeld: $I = (g_1, g_2)$ met $g_1 = x^2y$ en $g_2 = xy^2 - z$ in $\mathbb{Q}[x, y, z]$

$$xz \overset{?}{\in} I \qquad xz = y \cdot g_1 - x \cdot g_2$$

$$z^2 \overset{?}{\in} I \qquad z^2 = y^3 \cdot g_1 - (xy^2 + z) \cdot g_2$$

Strategie: " deel f door $g_1, \ldots, g_k$ met rest r "

$$f = q_1 g_1 + \ldots + q_k g_k + r$$

Voorbeeld: neem $f = xy$ en $g = x + y$

$$xy = y \cdot (x + y) - y^2, \qquad xy = x \cdot (x + y) - x^2$$

of $\quad xy = 0 \cdot (x + y) + xy \quad$?

Monomiale ordeningen

monoom = $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ (bijv. $x,\ \ y^2,\ \ x^2y^3z^5, \ldots$)

$$X < Y \iff \begin{cases} \deg(X) < \deg(Y), \text{ of} \\ \deg(X) = \deg(Y) \text{ en alfabetisch} \end{cases}$$

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < y^3 < \cdots$$

Gegeven $f = c_1X_1 + c_2X_2 + \cdots + c_rX_r$

met $X_1 > X_2 > \cdots > X_r$ en $c_i \neq 0$

- $\mathsf{LM}(f) = X_1$ **leidende monoom**
- $\mathsf{LC}(f) = c_1$ **leidende coëfficiënt**
- $\mathsf{LT}(f) = c_1X_1$ **leidende term**

Voorbeeld: $f = 2y^3 + xy^2 + 7$

$\mathsf{LM}(f) = y^3$ $\mathsf{LC}(f) = 2$ $\mathsf{LT}(f) = 2y^3$

f **reduceert** tot h modulo g

$$f \xrightarrow{g} h$$

als $\mathsf{LM}(g)$ een term T in f deelt, en

$$h = f - \frac{T}{\mathsf{LT}(g)} g$$

Voorbeeld:

$$xy \xrightarrow{y+x} xy - x \cdot (y + x) = -x^2$$

f **reduceert** tot h modulo $G = \{g_1, g_2, \ldots, g_k\}$

$$f \xrightarrow{G} h$$

als

$$f \xrightarrow{g_{i_1}} h_1 \xrightarrow{g_{i_2}} h_2 \xrightarrow{g_{i_3}} \cdots \xrightarrow{g_{i_{t-1}}} h_{t-1} \xrightarrow{g_{i_\ell}} h$$

Voorbeeld: $G = \{g_1, g_2\}$ met $g_1 = xy - y$ en $g_2 = y^2 - x$

$$xy^2 \xrightarrow{G} x \qquad \text{want} \qquad xy^2 \xrightarrow{g_1} y^2 \xrightarrow{g_2} x$$

f is **gereduceerd** modulo G als we f niet verder kunnen reduceren modulo G

$G = \{g_1, \ldots, g_k\}$ is een **Gröbner-basis** voor $I = (g_1, \ldots, g_k)$ als voor elke (niet-nul) $f \in I$ geldt dat $\mathrm{LM}(g_i) | \mathrm{LM}(f)$ voor een $g_i \in G$

Als $f \in I$ en $f \xrightarrow{G} r$ met r gereduceerd,
dan $r \in I$ en $\mathrm{LM}(g_i) \nmid \mathrm{LM}(r)$, dus $r = 0$

Oplossing ideale lidmaatschapsprobleem!

$f \in I$ dan en slechts dan als f reduceert tot 0
modulo een Gröbner-basis

Gevolg: Als G een Gröbner-basis is, is de rest r bij reductie van f modulo G uniek.

Bewijs: Stel $f \xrightarrow{G} r_1$ en $f \xrightarrow{G} r_2$ met r_1 en r_2 gereduceerd. Dan is $r_1 - r_2 = (f - r_2) - (f - r_1) \in I$ ook gereduceerd, en dus $r_1 - r_2 = 0$.

Wat kan er mis gaan?

$G = \{g_1, \ldots, g_k\}$ is **geen** Gröbner-basis als

$$f = \sum_{i=1}^{k} a_i g_i \qquad \text{met} \qquad \mathsf{LM}(g_i) \nmid \mathsf{LM}(f)$$

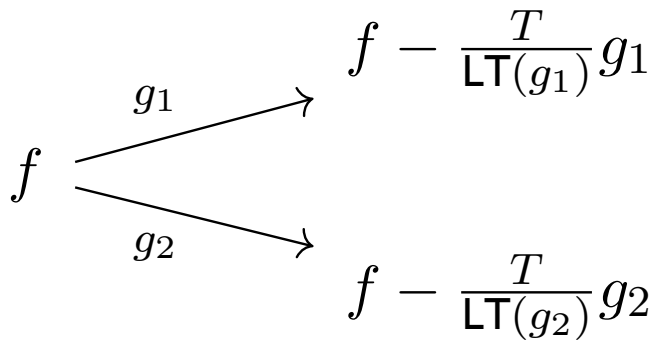
Als $g, h \neq 0$ polynomen en $L = \text{kgv}(\text{LM}(g), \text{LM}(h))$ dan

S-polynoom $$S(g,h) = \frac{L}{\text{LT}(g)}g - \frac{L}{\text{LT}(h)}h$$

Voorbeeld: $g = xy - y$ en $h = y^2 - x$, dan $L = \text{kgv}(xy, y^2) = xy^2$ en

$$S(g,h) = y \cdot g - x \cdot h = x^2 - y^2$$

Als term T van f deelbaar door $\mathsf{LM}(g_1)$ en $\mathsf{LM}(g_2)$, dan



$$\text{verschil} \;=\; \frac{T}{\mathsf{LT}(g_1)}g_1 - \frac{T}{\mathsf{LT}(g_2)}g_2 \;=\; \frac{T}{L}S(g_1, g_2)$$

Stelling van Buchberger: $G = \{g_1, \ldots, g_k\}$ is Gröbner d.e.s.d.a.

$$S(g_i, g_j) \xrightarrow{G} 0 \quad \text{voor elke } i, j$$

Algoritme van Buchberger

Input: $F = \{f_1, \ldots, f_k\}$

Output: Gröbner-basis $G = \{g_1, \ldots, g_\ell\}$ voor $I = (f_1, \ldots, f_k)$

- $G := F$ en $A := \{(f_i, f_j) : i < j\}$
- zolang $A \neq \varnothing$ neem $(g, h) \in A$ en bereken $S(g, h)$
- als $S(g, h) \xrightarrow{G} r \neq 0$ dan

$$G := G \cup \{r\}$$

$$\text{en } A := A \cup \{(g, r) : g \in G\}$$

Voorbeeld: $I = (f_1, f_2)$ met $f_1 = xy - y$ en $f_2 = y^2 - x$

$$S(f_1, f_2) = yf_1 - xf_2 = x^2 - y^2 \xrightarrow{f_2} x^2 - x =: f_3$$

$$S(f_1, f_3) = xf_1 - yf_2 = 0$$

$$S(f_2, f_3) = -x^3 + xy^2 \xrightarrow{f_3} xy^2 - x \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0$$

Conclusie: $G = \{f_1, f_2, f_3\}$ is Gröbner

Gröbner-basis $G = \{g_1, \ldots, g_k\}$ is **minimaal** als
$\mathsf{LC}(g_i) = 1$ en $\mathsf{LM}(g_j) \nmid \mathsf{LM}(g_i)$ voor $i \neq j$

Lemma: als $G = \{g_1, \ldots, g_k\}$ Gröbner en $\mathsf{LM}(g_2) \mid \mathsf{LM}(g_1)$ dan is $G' = \{g_2, \ldots, g_k\}$ ook Gröbner

Bewijs: als $\mathsf{LM}(g_1)|\mathsf{LM}(f)$ voor $f \in I$ dan ook $\mathsf{LM}(g_2)|\mathsf{LM}(f)$

(**Opgave**: bewijs dat $(g_2, \ldots, g_k) = I = (g_1, g_2, \ldots, g_k)$)

Lemma: als $G = \{g_1, \ldots, g_k\}$ en $H = \{h_1, \ldots, h_\ell\}$ minimale Gröbner-bases zijn voor I dan is $k = \ell$ en $\mathsf{LT}(g_i) = \mathsf{LT}(h_i)$ (mogelijk herindexeren)

Bewijs: $g_1 \in I$ en H is Gröbner, dus $\mathsf{LM}(h_1) | \mathsf{LM}(g_1)$.

Ook $h_1 \in I$ en G is Gröbner, dus $\mathsf{LM}(g_j) | \mathsf{LM}(h_1) | \mathsf{LM}(g_1)$,

dus $j = 1$ en $\mathsf{LM}(g_1) = \mathsf{LM}(h_1)$.

etc.

Gröbner-basis $G = \{g_1, \ldots, g_k\}$ is **gereduceerd** als minimaal en elke g_i is gereduceerd t.o.v. $G \backslash \{g_i\}$

Stelling: elk ideaal I heeft een unieke gereduceerde Gröbner basis

Bewijs: Stel G en H zijn gereduceerde Gröbner-bases (dus $\mathrm{LT}(g_i) = \mathrm{LT}(h_i)$), en stel dat $g_i \neq h_i$.

Dan $0 \neq g_i - h_i \in I$, dus $\mathrm{LM}(g_j) | \mathrm{LM}(g_i - h_i)$ voor een j.

Maar dan deelt $\mathrm{LM}(g_j) = \mathrm{LM}(h_j)$ een term van g_i of h_i, dus G of H is niet gereduceerd.

Voorbeeld: $I = (f, g)$ met $f = y^2 + 2$ en $g = xy - y$

Buchberger:

$$S(f, g) = y^2 + 2x \xrightarrow{f} 2x - 2 =: h$$

$$S(f, h) = y^2 + 2x \xrightarrow{h} 0$$

$$S(g, h) = 0$$

$\{f, g, h\}$ is een Gröbner basis voor I

Minimaliseren: $\mathrm{LM}(h) = x$ deelt $\mathrm{LM}(g) = xy$, dus gooien g weg

$\{y^2 + 2, x - 1\}$ is minimale Gröbner basis voor I

Reduceren: $y^2 + 2$ is gereduceerd t.o.v. $x - 1$ en vice versa

$\{y^2 + 2, x - 1\}$ is gereduceerde Gröbner basis voor I

Toepassingen

- ideale lidmaatschapsprobleem
- unieke representatie f mod I
- basis voor $\mathbb{Q}[x_1, \ldots, x_n]/I$ als $\mathbb{Q}$-vectorruimte
- ideaal gelijkheid $I \stackrel{?}{=} J$
- radicaal lidmaatschap $f \stackrel{?}{\in} \sqrt{I}$
- voortbrengers vinden van kern $\varphi : \mathbb{Q}[y_1, \ldots, y_m] \to \mathbb{Q}[x_1, \ldots, x_n]$
- kleuren van grafen
- nog veel meer!